UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

SILVER FERN CHEMICAL, INC., a Washington corporation,

Plaintiff,

v.

SCOTT LYONS, an individual; TROY KINTO, an individual; KING HOLMES, an individual; ROWLAND MORGAN, an individual; and AMBYTH CHEMICAL COMPANY, a Washington corporation,

Defendants.

CASE NO. 2:23-cv-00775-TL

ORDER ON MOTION TO DISMISS

This is an action for damages and injunctive relief for the misappropriation of trade secrets, breach of contract, and other related claims. This matter is before the Court on Defendants' Motion to Dismiss. Dkt. Nos. 45 (motion), 49-1 (praecipe). Having reviewed Plaintiff's response (Dkt. No. 47), Defendants' reply (Dkt. No. 48), and the relevant record, and finding oral argument unnecessary, *see* Local Civil Rule 7(b)(4), the Court GRANTS IN PART and DENIES IN PART the motion with leave to amend.

I. BACKGROUND

A. Factual Background

Plaintiff Silver Fern Chemical, Inc., is a chemical distribution company based in Seattle, Washington. Dkt. No. 7 (sealed complaint) ¶¶ 1, 9. Defendants Scott Lyons, Troy Kinto, and King Holmes are former employees and salespeople of Plaintiff and current employees of Defendant Ambyth Chemical Company, also based in Seattle. *Id.* ¶ 1, 10–12, 14. Defendant Rowland Morgan is the operator of Defendant Ambyth. *Id.* ¶¶ 13, 68.

The general background of this matter was detailed in the Court's Order denying Plaintiff's motion for a temporary restraining order ("TRO"). *See* Dkt. No. 40 at 2–3. The Court recites below the factual allegations relevant to the instant motion, as alleged by Plaintiff in the Complaint.

1. Trade Secrets

Plaintiff has spent years and millions of dollars building customer relationships. Dkt. No. 7 ¶ 24. To maintain relationships and serve its customers, Plaintiff collects and maintains extensive information regarding each customer's needs and how that customer conducts business: product needs and specifications, timing needs, delivery needs, the employees and owners who handle a diverse range of responsibilities for the customer, and contact information for the point person that purchases its chemicals. *Id.* ¶¶ 26, 28, 31.

Plaintiff also invests a lot of employee time and money to evaluate each of its vendors, and to ensure the quality and unique specifications of the chemicals that each vendor supplies. *Id.* ¶¶ 33–34. This information includes evaluations of risk in working with a prospective vendor, the outcomes of those relationships, the vendor's products, and details about the vendor's manufacturing, logistics, and business practices. *Id.* ¶¶ 35, 43. Plaintiff also engages in a long and labor-intensive process of vendor and product qualification with any given customer. *Id.*

¶ 41. This process includes providing samples and documentation to the customer, and can involve layers of technical, regulatory, and quality assessments regarding the specific product and specific manufacturer. *Id.* ¶ 41.

Plaintiff's customer and vendor information is maintained in two main password-protected databases and under multiple layers of access and password restrictions. *Id.* ¶¶ 29, 61(f)–(h). Employees are required to acknowledge confidentiality requirements and to sign a separate Confidentiality Agreement. *Id.* ¶ 63. The information Plaintiff seeks to protect is not generally known, and Plaintiff has invested millions of dollars in collecting, analyzing, and storing this information for its sole economic benefit. *Id.* ¶¶ 64–65.

2. Computer Activity

Between January 17 and April 17, 2023, Defendants Holmes, Kinto, and Lyons attempted to "permanently delete" thousands of items from their email mailboxes with Plaintiff. Dkt. No. 7 ¶¶ 92–94. A large portion of those items were deleted on April 14, their last day of employment. *Id.* However, during this period, Defendants' email accounts were on a litigation hold, meaning that their deleted items were not, in fact, permanently deleted. *Id.* ¶ 96. Defendants did not have a legitimate business purpose for attempting to delete the items. *Id.* ¶ 95. Plaintiff specifically advised its employees—including multiple times during Defendants' employment—that emails were company property and should not be deleted. *Id.*

B. Procedural History

On May 24, 2023, Plaintiff filed the instant action. Dkt. Nos. 1, 7 (sealed). On June 2, the Court denied Plaintiff's motion for a TRO. Dkt. No. 40. On June 14, Defendants filed the instant motion to dismiss all federal claims and the remaining state claims for lack of subject matter jurisdiction. Dkt. Nos. 45, 49-1; *see also* Dkt. No. 48 (reply). Plaintiff opposes. Dkt. No. 47.

II. LEGAL STANDARD

A defendant may seek dismissal when a plaintiff fails to state a claim upon which relief can be granted. Fed. R. Civ. P. 12(b)(6). In reviewing a Rule 12(b)(6) motion to dismiss, the Court takes all well-pleaded factual allegations as true and considers whether the complaint "state[s] a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). While "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements" are insufficient, a claim has "facial plausibility" when the party seeking relief "pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 672. "When reviewing a dismissal pursuant to Rule . . . 12(b)(6), 'we accept as true all facts alleged in the complaint and construe them in the light most favorable to plaintiff[ ], the non-moving party.'" *DaVinci Aircraft, Inc. v. United States*, 926 F.3d 1117, 1122 (9th Cir. 2019) (alteration in original) (quoting *Snyder & Assocs. Acquisitions LLC v. United States*, 859 F.3d 1152, 1156–57 (9th Cir. 2017)).

III. DISCUSSION

Defendants argue that Plaintiff has not stated a federal claim under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, or for misappropriation of trade secrets under the Defend Trade Secrets Act ("DTSA"), 18 U.S.C. § 1836 *et seq.*, and the analogous state law, the Washington Uniform Trade Secrets Act ("WUTSA"), RCW 19.108.010 *et seq. See* Dkt. No. 49-1 at 9-17; Dkt. No. 48 at 5–15. Defendants further argue that the Court should decline to exercise supplemental jurisdiction over the remaining state-law claims. *See* Dkt. No. 49-1 at 17; Dkt. No. 48 at 15–16. Plaintiff opposes on all grounds. *See* Dkt. No. 47.

A. First Cause of Action: CFAA

Plaintiff alleges that Defendants Lyons, Kinto, and Holmes "permanently deleted" company emails, even after Plaintiff instructed them not to delete emails. *See* Dkt. No. 7 ¶¶ 91–96, 130–33. Defendants argue that these allegations do not state a claim under the CFAA because Plaintiff does not allege that these Defendants exceeded their authorization to access the information. *See* Dkt. No. 49-1 at 9–11; Dkt. No. 48 at 5–7. Plaintiff responds that the Defendants "utilized their authorized access to unlawfully alter—i.e., *delete*—information that they were not entitled to delete." Dkt. No. 47 at 15.

The CFAA states in relevant part:

> Whoever . . .
>
> > knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period . . .
>
> shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030(a)(4); *see also* 18 U.S.C. § 1030(g) (creating private right of action).

To bring a private action under § 1030(a)(4), a plaintiff must show that a defendant: "(1) accessed a 'protected computer,' (2) without authorization or exceeding such authorization that was granted, (3) 'knowingly' and with 'intent to defraud,' and thereby (4) 'further[ed] the intended fraud and obtain[ed] anything of value,' causing (5) a loss to one or more persons during any one-year period aggregating at least $5,000 in value." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132 (9th Cir. 2009). "The statute thus provides two ways of committing the crime of improperly accessing a protected computer: (1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly." *Facebook,*

Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1066 (9th Cir. 2016) (quoting *Musacchio v. United States*, 577 U.S. 237, 240 (2016)).

"The term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). "As this definition makes clear, an individual who is authorized to use a computer for certain purposes but goes beyond those limitations is considered by the CFAA as someone who has 'exceed[ed] authorized access.'" *Brekka*, 581 F.3d at 1133. "'[E]xceeds authorized access' is limited to violations of restrictions on *access* to information, and not restrictions on its *use*." *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (en banc) (emphases in original); *see also Van Buren v. United States*, 141 S. Ct. 1648, 1662 (2021) ("[A]n individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him.").

Here, the Court finds that Plaintiff has not stated a claim under the CFAA. Plaintiff essentially alleges that Defendants Lyons, Kinto, and Holmes violated a use restriction imposed by Plaintiff—that is, deletion of emails in violation of company policy, which amounts to "altering" information that they were not entitled to delete. *See* Dkt. No. 7 ¶¶ 92–96; Dkt. No. 47 at 15. But this argument is squarely foreclosed by *Nosal* and *Van Buren*, in which both the Ninth Circuit and the United States Supreme Court rejected Plaintiff's understanding of the CFAA.

In *Nosal*, employees of an executive search firm were authorized to access a computer database of confidential information, but they downloaded and transferred information to the defendant in violation of a company policy forbidding disclosure of confidential information. 676 F.3d at 856. In a prosecution under 18 U.S.C. § 1030(a)(4), the government argued (among other things) that the word "so" in 18 U.S.C. § 1030(e)(6) means "in that manner," which would

refer to "use restrictions." *Nosal*, 676 F.3d at 857. The court found that Congress enacted the CFAA "primarily to address the growing problem of computer hacking" and that the phrase "exceeds unauthorized access" thus would apply not to persons who use a computer for an unauthorized purpose, but rather to "individuals whose initial access to a computer is authorized but *who access unauthorized information or files*." *Id.* (emphasis added). Notably, the court observed that "[e]mployer-employee and company-consumer relationships are traditionally governed by tort and contract law," but the government's proposed interpretation "allows private parties to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law." *Id.* at 860.

Similarly, in *Van Buren*, a police sergeant was authorized to access a law enforcement computer database, but he ran a license-plate search in exchange for money in violation of department policy. 141 S. Ct. at 1653. In a prosecution under 18 U.S.C. § 1030(a)(2), which relies on the same statutory definition of "exceeds authorized access" at issue here, 18 U.S.C. § 1030(e)(6), the government argued (as it did in *Nosal*) that the defendant was not "entitled [ ] to obtain" the records at issue. *Van Buren*, 141 S. Ct. at 1654. Like the Ninth Circuit, the Supreme Court rejected the government's interpretation as inconsistent with the statutory text, context, and structure, as well as leading to far-reaching (and undesirable) consequences. *Id.* at 1654–62. Notably, the Supreme Court described CFAA liability as "a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system." *Id.* at 1658–59.

Nosal and *Van Buren* are materially indistinguishable from this matter. There is no dispute that Defendants Lyons, Kinto, and Holmes had authorization to access their company emails when they did (*compare* Dkt. No. 49-1 at 11, *with* Dkt. No. 47 at 15), just as the employees in *Nosal* had authorization to access the confidential database, 676 F.3d at 856, and

just as the sergeant in *Van Buren* had authorization to access the law enforcement database, 141 S. Ct. at 1653. Further, Plaintiff states the "gravamen" of its complaint is that the Defendants *altered* (*i.e.*, deleted) information that they were not entitled to delete under company policy (Dkt. No. 47 at 15), just as the employees in *Nosal* (and the defendant-recipient) were alleged to have *obtained* (*i.e.*, downloaded and transferred) information they were not entitled to transfer under company policy, and just as the sergeant in *Van Buren* was alleged to have *obtained* (*i.e.*, searched database for) information he was not entitled to access under department policy.[1] Thus, like the defendants in *Nosal* and *Van Buren*, Defendants are not liable under the CFAA for either obtaining information that they were otherwise authorized to access or for allegedly misusing that information. *See also, e.g.*, *United Fed'n of Churches, LLC v. Johnson*, 598 F. Supp.3d 1084, 1095 n.8 (W.D. Wash. 2022) (holding defendants did not exceed authorized access where there was "no allegation that Defendants obtained or altered information from areas of [a website] beyond their authorized *access*" (emphasis added)). Therefore, Plaintiff's CFAA claim will be dismissed.

However, Plaintiff offers to amend its complaint to state a claim under a different provision of the CFAA, 18 U.S.C. § 1030(a)(5)(A). *See* Dkt. No. 47 at 15 n.2 (citing *1-800 Remodel, Inc. v. Bodor*, No. C18-472, 2018 WL 6340759, at *7 (C.D. Cal. Oct. 17, 2018) and *United States v. Grupe*, No. CR17-90, 2018 WL 775358, at *3 (D. Minn. Feb. 8, 2018)). Defendants oppose granting leave to amend, arguing that Plaintiff "cannot cure its deficiencies" because "the emails were not, in fact, deleted" (citing Dkt. No. 7 ¶ 96) and that Plaintiff "already

[1] Plaintiff protests that Defendants cite no cases involving *deletion* of data (as opposed to downloads and transfers). *See* Dkt. No. 47 at 15–16. This distinction is unavailing, as "obtain" and "alter" are textually located in the same part of the statute. *See* 18 U.S.C. § 1030(e)(6).

declined an opportunity to amend."[2] Dkt. No. 48 at 7. But Defendants cite no authorities for their argument that Plaintiff cannot cure. Without the benefit of a proper pleading and full briefing on a motion to dismiss, the Court cannot say at this early stage that amendment would be futile.

Accordingly, as to Plaintiff's CFAA claim, Defendants' motion is GRANTED with leave to amend.

B. Fourth and Fifth Causes of Action: DTSA & WUTSA

Plaintiff alleges that its subject trade secrets are "its compilation of information related to its customers and vendors." Dkt. No. 47 at 17; *see* Dkt. No. 7 ¶¶ 1–44, 147–74. Defendants argue only that Plaintiff has not described the trade secrets with sufficient particularity, instead offering "impermissible conclusory allegations" with "vague" and "nonspecific" references.[3] *See* Dkt. No. 49-1 at 11–16; Dkt. No. 48 at 9–11. Defendants also briefly argue that Plaintiff has not sufficiently alleged knowledge or acquisition of trade secrets by Defendants Morgan or Ambyth. *See* Dkt. No. 49-1 at 16–17. Plaintiff opposes. *See* Dkt. No. 47 at 17–26.

The DTSA defines "trade secret" as

> all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

[2] Defendants certify that prior to filing this motion, they offered to withdraw the motion and stipulate to an amendment, but Plaintiff did not accept the offer. *See* Dkt. No. 48 at 18. Going forward, the Court expects the Parties to work together to resolve disputes efficiently and thus conserve judicial resources.

[3] "Defendants do not disagree that '[c]ompliations of customer information *may* be a trade secret.' " Dkt. No. 48 at 8 (quoting *Robbins, Geller, Rudman & Dowd, LLP v. State*, 328 P.3d 905, 911 (Wash. Ct. App. 2014) (emphasis in original)).

Further, in their reply, Defendants raise new arguments regarding *other* aspects of Plaintiff's misappropriation claims, such as the confidentiality of the subject information and evidence of misconduct. *See* Dkt. No. 48 at 9, 12–15. Defendants did not move for dismissal on these grounds. "The district court need not consider arguments raised for the first time in a reply brief." *Zamani v. Carnes*, 491 F.3d 990, 997 (9th Cir. 2007). Therefore, the Court will disregard these arguments.

> (A) the owner thereof has taken reasonable measures to keep such information secret; and
>
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

18 U.S.C. § 1839(3); *see also* 18 U.S.C. 1836(b)(1) (creating private right of action).

Similarly, the WUTSA defines trade secret as

> information, including a formula, pattern, compilation, program, device, method, technique, or process that:
>
> > (a) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and
> >
> > (b) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

RCW 19.108.010(4); *see also* RCW 19.108.030–19.108.040 (establishing remedies).

"Under either statute, '[t]herefore, the definition of trade secret consists of three elements: (1) information, (2) that is valuable because it is unknown to others, and (3) that the owner has attempted to keep secret.'" *Genasys Inc. v. Vector Acoustics, LLC*, 638 F. Supp. 3d 1135, 1151 (S.D. Cal. 2022) (analyzing DTSA and California's version of the Uniform Trade Secrets Act, substantially similar to the WUTSA) (quoting *InteliClear, LLC v. ETC Glob. Holdings, Inc.*, 978 F.3d 653, 657 (9th Cir. 2020)). "Although the complaint need not 'spell out the details of the trade secret,' a plaintiff seeking relief for trade secret misappropriation must identify the trade secret 'with sufficient particularity . . . to permit the defendant to ascertain at least the boundaries within which the secret lies.'" *Bombardier Inc. v. Mitsubishi Aircraft Corp.*, 383 F. Supp. 3d 1169, 1178 (W.D. Wash. 2019) (quoting *SMS Signature Cars v. Connects Mktg. LLC*, No. C12-1300, 2012

WL 12893935, at *2 (C.D. Cal. Oct. 29, 2012)). "The relevant portions of the DTSA and [W]UTSA are almost identical," and thus they can be analyzed together. *Id.*

Finally, this Court has held that "*at the motion to dismiss stage*, 'a plaintiff should not be compelled to divulge with specificity all of its possible trade secrets . . . in order to proceed to discovery.'" *RealD Spark LLC v. Microsoft Corp.*, No. C22-942, 2023 WL 3304250, at *3 (W.D. Wash. May 8, 2023) (emphasis in original) (quoting *T-Mobile USA, Inc. v. Huawei Device USA, Inc.*, 115 F. Supp. 3d 1184, 1193 (W.D. Wash. 2015)). "In a trade secret case, a plaintiff should not be expected to publicly disclose the details that would expose—and therefore, destroy—the trade secret in order to begin a case. Therefore, it is ordinarily sufficient for a plaintiff to provide descriptions of the categories of the asserted trade secrets in a complaint." *Id.* (citing The Sedona Conference, *The Sedona Conference Commentary on the Proper Identification of Asserted Trade Secrets in Misappropriation Cases*, 22 Sedona Conf. J. 223, 248 (2021)).

Here, the Court finds that Plaintiff has described its trade secrets with sufficient particularity to state a claim under the DTSA and WUTSA. Plaintiff essentially pleads that its compilations of customer and vendor information are its trade secrets. Dkt. No. 7 ¶¶ 23–66; *see also* Dkt. No. 47 at 9–11. Plaintiff explains that it collects and maintains information on customer needs "and how that customer conducts business: its product needs and specifications, its timing needs, its delivery needs, the employees and owners who handle a diverse range of responsibilities for the customer, and more." Dkt. No. 7 ¶ 26; *see also id.* ¶ 31 (describing its "compilation of customer data" as including "confidential information regarding customers' products, timing, delivery needs, and much more"); *id.* ¶¶ 61(f)–(g) (detailing contents of "Salesforce Database" and "Customer information files," including approved manufacturers and products, requirements, special requests, and more). Similarly, Plaintiff alleges that it collects and maintains information about its vendors, including assessments of risk in working with a

particular vendor (*id.* ¶ 35), confidential information about their products (*id.* ¶ 43), and "details about their manufacturing, logistics and business practices" (*id.*). *See also id.* ¶¶ 61(f), (h) (detailing contents of "Salesforce Database" and "Vendor information files," including detail of products offered, pricing, certifications and guarantees, and more).

Plaintiff's descriptions of its customer and vendor information are sufficient to permit Defendants to ascertain the boundaries within which the trade secrets lie. *Bombardier*, 383 F. Supp. 3d at 1178; *see NW Monitoring LLC v. Hollander*, 534 F. Supp. 3d 1329, 1336–37 (W.D. Wash. 2021) (at motion-to-dismiss stage, holding allegation of "customer pricing information" was sufficient to identify trade secret); *Bite Tech Inc. v. X2 Impact, Inc.*, No. C12-1267, 2012 WL 13018749, at *4 (W.D. Wash. Dec. 21, 2012) (at motion-to-dismiss stage, holding allegations of disclosures to plaintiff "regarding [defendant's] technology, research and development, future products, business plans and business partners" was sufficient to identify trade secret in impact sensing technology); *Albert's Organics, Inc. v. Holzman*, 445 F. Supp. 3d 463, 473 (N.D. Cal. 2020) (at motion-to-dismiss stage, holding allegations of customer information including "names of [plaintiff's] customers and suppliers," "pricing and financial resources," and "key confidential business relationships" were sufficient to identify trade secret); *cf. Brocade Commc'ns Sys., Inc. v. A10 Networks, Inc.*, 873 F. Supp. 2d 1192, 1214 (N.D. Cal. 2012) (denying defendant's motion for summary judgment on particularity of trade secret where defined to include "confidential customer-related information including customer lists and contact information, pricing guidelines, historical purchasing information, and customers' business needs/preferences").

Defendants' authorities are distinguishable. *See* Dkt. No. 49-1 at 13–15. In *Vendavo, Inc. v. Price f(x) AG*, the alleged categories of trade secrets were more varied and swept more broadly than they do here. No. C17-6930, 2018 WL 1456697, at *3 (N.D. Cal. Mar. 23, 2018) (alleging

theft of customer and vendor information, but also, *inter alia*, "source code," "marketing plans and strategic business development initiatives," and "other information related to the development of its price-optimization software"). In *Genasys*, the plaintiff did not explain "how and why" the categories of information (including client data and pricing information) were protected trade secrets, instead relying on "conclusory buzzwords." 638 F. Supp. 3d at 1151–52. In both *Olson Kundig, Inc. v. 12th Avenue Iron, Inc.* and *Synopsys, Inc. v. ATopTech, Inc.*, trade secret allegations arose in the context of product design where identification of specific components would be needed. No. C22-825, 2022 WL 4534422, at *8 (W.D. Wash. Sept. 28, 2022); No. C13-2965, 2013 WL 5770542, at *6 (N.D. Cal. Oct. 24, 2013). While *Multifab, Inc. v. Zweiger* involved customer information, the case turned on whether a trade secret existed in a *single* customer's information when the customer's identity was already known. No. C19-6164, 2020 WL 2614736, at *4 (W.D. Wash. May 22, 2020). And while *CAE Integrated, LLC v. Moov Technologies Inc.* involved customer identities, the case turned on whether the customer list at issue qualified as a trade secret given the bounded nature of the relevant industry. No. C21-377, 2021 WL 6497092, at *4–5 (W.D. Tex. Dec. 22, 2021).

The Court makes no comment on whether the subject information is ultimately a protected trade secret, or whether this level of particularity will be sufficient at later stages of this litigation. But Defendants are currently on notice that information about the needs and offerings of Plaintiff's customers and vendors are the alleged secrets—categories of information that should be readily familiar to a firm in the chemical distribution industry. It is difficult to imagine greater particularity without requiring Plaintiff to divulge the very compilations at issue.

The Court also finds that at this stage, Plaintiff has stated a claim of misappropriation against Defendants Morgan and Ambyth. Defendants offers only four sentences of argument (with no authorities) that Plaintiff makes a "speculative leap" between the alleged facts and these

Defendants' liability. *See* Dkt. No. 49-1 at 16–17. The argument is buried at the end of a seven-page section nominally about the particularity of trade secrets. *See id.* at 11–17. It is thus little surprise that Plaintiff does not address the argument in its response. Regardless, Plaintiff pleads that Defendants Lyons, Kinto, and Holmes had communications with Defendants Morgan and Ambyth not long before their departure from Plaintiff (Dkt. No. 7 ¶¶ 67–77) and that some of Plaintiff's customers made or attempted communications with Defendants after their departure from Plaintiff (*id.* ¶¶ 113–25), all of which plausibly allege that Defendants Morgan and Ambyth encouraged or conspired to commit the alleged misappropriation of trade secrets.

Accordingly, as to Plaintiff's trade secrets claims, Defendants' motion is DENIED.

C. Supplemental Jurisdiction

Finally, Defendants argue that if no legally sufficient federal claims remain in this matter, the Court should decline supplemental jurisdiction over Plaintiff's state law claims. *See* Dkt. No. 49-1 at 17; Dkt. No. 48 at 15–16. Plaintiff opposes. *See* Dkt. No. 47 at 26–28.

As discussed above, the Court will allow Plaintiff to replead its CFAA claim and will not dismiss Plaintiff's trade secrets claims. Therefore, the Court will retain jurisdiction over Plaintiff's state law claims. *See* 28 U.S.C. § 1367(c).

IV. CONCLUSION

Accordingly, Defendants' Motion to Dismiss (Dkt. Nos. 45, 49-1) is GRANTED IN PART and DENIED IN PART. Plaintiff's CFAA claim is DISMISSED with leave to amend. Should Plaintiff choose to amend, the amended complaint should be filed **within thirty (30) days** of this Order.

Dated this 19th day of December 2023.

Tana Lin
United States District Judge